(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 November 2001 (15.11.2001)

PCT

(10) International Publication Number
WO 01/86599 A2

(51) International Patent Classification[7]: G07F 7/00

(21) International Application Number: PCT/IB01/00809

(22) International Filing Date: 13 April 2001 (13.04.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/197,775 14 April 2000 (14.04.2000) US
60/264,013 26 January 2001 (26.01.2001) US

(71) Applicant *(for all designated States except US)*: **SUPER-COM LTD.** [IL/IL]; Hataas Street 25, New Industrial Area, 44425 Kfar Saba (IL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **LANDMAN, Avi** [IL/IL]; 99 Hagdud Haivri Street, 26306 Kiriat Haim (IL). **ROZEN, Eli** [IL/IL]; 38 Heleni Hamalka Street, 46768 Herzliya Pituah (IL). **HASSAN, Jacob** [IL/IL]; 21 Shnat Hayovel Street, 45304 Hod Hasharon (IL).

(74) Agent: **BEN-DAVID, Yirmiyahu, M.**; Jeremy M. Ben-David & Co. Ltd., P.O. Box 4508, Har Hotzvim Hi-Tech Park, 91450 Jerusalem (IL).

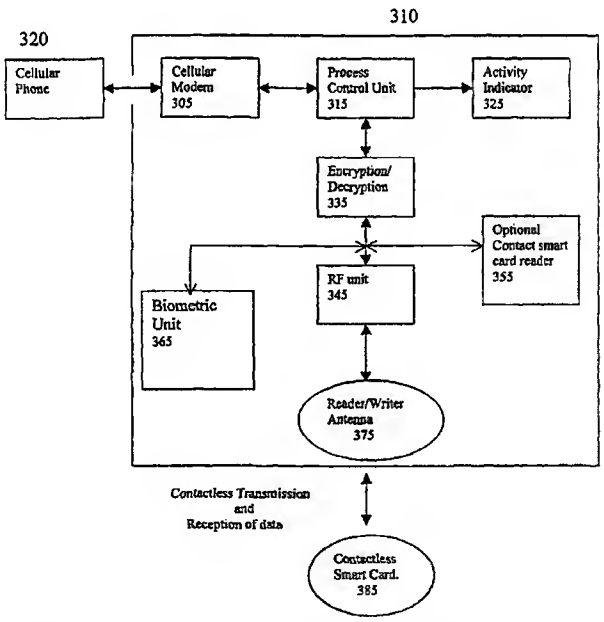
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *without international search report and to be republished upon receipt of that report*

[Continued on next page]

(54) Title: SMART COMMUNICATIONS



(57) Abstract: A method and apparatus for providing a wireless device with the ability to have secure e-commerce transactions utilizing a contactless smart card. Additionally, the method and apparatus provide for a wireless smart card transaction system which utilizes biometric identification methods. The system may incorporate at least one biometric input device, such as a fingerprint reader, a camera or micro-camera for iris or face recognition, and/or a standard microphone for voice recognition or any other biometric input device.

WO 01/86599 A2

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

SMART COMMUNICATIONS

This application claims the benefits of United States Provisional Application Nos. 60/197,775, filed April 14, 2000, and 60/264,013, filed January 26, 2001, which are co-pending and are hereby incorporated by reference.

BACKGROUND OF THE INVENTION

1. Field of the Invention

This invention relates to wireless communications, and more particularly, to a system suitable to utilize smart card technology with a wireless communication device to provide authorization and security features for wireless communications and transactions.

In addition, the present invention relates generally to the field of authentication of electronic transactions, and more particularly to a non-reputable digital signature that allows authentication of the identity of a user/customer by comparison with an unique biological indicia.

2. Description of the Related Technology

Cellular phones are well known in the prior art. For example, U.S. Patent No. 5,867,795 shows a portable electronic device including a virtual image display positioned within a housing or remote unit. The device is capable of providing an image of information contained on a smart card as well as transactions processed in response to

data transmitted by a two-way voice transceiver between a host database and the portable electronic device. In addition, the above-referenced aptent shows a sensor constructed to have the smart card positioned adjacent thereto in data sensing juxtaposition and electronics connected to the sensor for processing data between the host database and the portable electronic device, and for reading and writing data to the smart card.

US Patent No. 5,821,983 shows a smart card, a non-passive, secure microprocessor-based data storage medium, is used for the storage of a plurality of data messages and is read by a video telephone terminal equipped with a smart card reader to provide transmission of a data message, comprising video image data, either in still frame or full motion format, to a remote video telephone terminal. The use of the smart card for storage of a data message provides a secure, transportable message that is available for transmission from any video telephone terminal having smart card reading capability.

Smart cards are non-passive data storage devices which comprise a microprocessor, memory and I/O circuitry. Smart cards are generally used when a secure and portable means to store data is desired. There are contactless smart cards which do not require physical contact to transfer data between the card and a card reader. There are also smart cards which have electrical contacts to facilitate such data transfer. Prior art U.S. Patent No. 4,480,178 describes a contactless smart card, and U.S. Patent No. 5,120,939 describes the security which smart cards provide when used as data memory devices.

Electronic commerce is a widespread means of conducting business. The Internet and World Wide Web have created new avenues for conducting business. Electronic

business transactions present a number legal and financial problems. These electronic transactions create security concerns because the data is transmitted across public networks and can be intercepted. Encryption methods have been developed which allow data to be read only by the designated receiver. For example, public key encryption allows a first user to send a message to a second user that is encrypted using the second user's public key. The second user's public key can be freely distributed to anyone the second user wishes to communicate with. The message can only be decrypted using the second user's private key. If the message is intercepted it cannot be decoded without the second user's private key.

The identity of a party transmitting a message executing an electronic transaction is also of concern, particularly where one of the parties is obliged to perform in the future or is subject to some future liability. In such transactions it is necessary that the parties not be able to repudiate the agreement. Also, the identity of the parties must be clearly established so that each can be assured that the other party is in fact the person it represents to be, and is able to perform. Further, the identity of the parties may need to be established with a high degree of certainty to support a legal claim, should one of the parties later attempt to avoid or repudiate the transaction.

Digital signatures have been developed to provide a means for identifying a party transmitting an electronic message. One method for creating digital signatures is to generate public and private key pairs for each of a group of parties that may wish to exchange digitally signed documents. Each of the parties stores its public decrypting keys in a registry along with identifying information, such as the key owner's name and e-mail

address. The key owners each keep their private encrypting keys secret.

To create a digital signature a party encrypts a message with his private encrypting key that includes the same identifying information that is stored in the registry. The party receiving the encrypted message goes to the registry and retrieves the sending party's public decrypting key and identifying information. The receiving party decrypts the message using the decrypting key from the registry and extracts the identifying information. If the identifying information found in the message matches the information stored in the registry then the receiving party concludes that the message is genuine. Further, there is some assurance that the sending party will not deny that he sent the message since only the sending party's private encrypting key can create a message that the sending party's public decrypting key can decode.

Known digital signature techniques suffer from certain problems. A third party may intercept a signed message and use the signed message to spoof another party. By retransmitting the signed message, the interceptor may be able to convince a recipient that he is the true sender. This is the so-called "man-in-the-middle" attack.

In addition, known digital signatures are subject to repudiation. A party may no longer wish to be bound by a disadvantageous agreement or may be subject to criminal or civil liability if he made the agreement. That party may simply deny sending a particular message. The party may claim that he did not intend to execute a transaction with a particular party but was instead the victim of a man-in-the-middle attack.

With known digital signature techniques, the only information connecting the sender with the message is the database entry in the registry containing his public decrypting key and the identifying information. Thus, the sender may repudiate a

transaction by claiming that his public decrypting key was registered without his authority.

SUMMARY OF THE INVENTION

An object of the invention is to provide a wireless device with the ability to have secure e-commerce transactions utilizing a contactless smart card. It is a further object of the present invention to provide a wireless smart card transaction system which utilizes biometric identification methods. The system may incorporate at least one biometric input device, such as a fingerprint reader, a camera or micro-camera for iris or face recognition, standard microphone for voice recognition or any other biometric input device.

Another object of the invention to is to capture the biometric data of a person using the device/module. Once the biometric data has been captured, another object of the invention is to encrypt the biometric data and transmit it to a remote host or server for authorization. Alternatively, the device/module may perform a local authorization of the biometric data. After the device/module has performed the local authorization, the device may transmit an encrypted authorization message to a host or service supplier. If either authorization method fails to approve of a user, the device may deny the user services.

Another object of the invention is to provide a financial information and transaction system which utilizes wireless communications. In this system, a device is connected to a financial institution via a wireless connection. Smart cards are utilized to verify authorization for communications and transactions, thereby minimizing potential security problems which could otherwise result from use of a wireless device. Alternatively, a smart card is advantageously utilized not only for authorization, but also

to maintain a secure record of available funds. The system not only provides the functionality of an ATM network, but also provides non-financial services, thereby forming an integrated system.

In another embodiment, a wireless communication device may be comprised of a communications interface and a contactless smart card interface, such as a contactless reader/writer, connected to the communications interface. The communications interface may include a controller, transmission/reception subsystem, and/or user interface. The controller may be a microprocessor and the user interface may include a microphone, speaker, key pad/board, micro-camera, display screen, touch screen or any other input/output device.

An object of the invention is to provide a module to upgrade existing wireless devices to include a smart card reader/writer, in particular a contactless smart card reader/writer, in order to communicate with contactless cards.

It is a further object of the invention to provide a smart card transaction system which is integrated with wireless communication devices, including personal digital assistants (PDAs), cellular phones, PCS systems, pagers, etc. The format of the wireless communication is not a limitation to the system. It is a further object of the invention to provide smart card based transactions and token redemption systems. It is a further object of the invention to provide enhanced security to such systems through biometric authentication processes and apparatus. It is a further object of the invention to provide a transaction system integrated with a wireless communication system utilizing either contact based or contactless smart card technologies.

According to an advantageous feature of the invention, a wireless communication

device such as a cellular phone may be utilized to access a communication network. A transaction may be conducted over the communication network, and a token or other indicia of value may be transmitted to the wireless communication device. The wireless communication device may then download the token, or other indicia of value, or other information to a smart card via integrated or add-on contact based or contactless smart card interfaces (such as a reader/writer). The transaction system may include one-to-one security/authentication features or one-to-many security/authentication features, when involving a remote host computer database storage.

In another embodiment, a module may include a contact smart card reader. The module may be used with contact smart cards, contactless smart cards, or both.

These, together with other objects and advantages which will be subsequently apparent, reside in the details of construction and operation as more fully hereinafter described in the claims, with reference to the accompanying drawings forming a part thereof, wherein like numerals refer to like elements throughout.

The present invention is directed to methods and apparatus for storing a digital signature, analzing a "live" signature and comparing the two to provide positive user authentication and non-repudiation. It is an object of the present invention to store a unique characteristic of the sender, such as biological indicia that can only have come from the user. In a perferred embodiment, a digital signature is stored in the memory of a bioauthentication smart card for comparison to a "live" signature.

Another object of the present invention is to store a digital signature that allows positive identification of the sender which cannot be repudiated.

Another object of the present invention is to analyze a stored digital signature

with a real time signature applied to a smart card.

Another object of the present invention is to provide a method for positively identifying a user during an electronic transaction with a biologically-based digital indicia.

The present invention is directed to methods and apparatus for creating and storing a digital for use in electronic commerce. The person requesting the electronic transaction

digital certificate such that the digital certificate provides positive identification of the sender and minimizes the ability of the sender to repudiate the authenticity of the certificate and any transaction embodied in an electronic document appended to the certificate.

According to an aspect of the present invention, a person, hereinafter called a user, wishing to obtain a bioauthentication smart card visits a local bank or service center and enters a data corresponding to a biological or physical characteristic of himself, for example, his signature into a smart card. Preferably, the data is entered in digital form, but could be entered by optical imaging (e.g. a photograph or a scanned fingerprint, iris, or retina) which is then processed into digital form. The digital representation of the registrant's biological indicia is encrypted using the registrant's private key and sent to the certificate authority along with the registrant's public key. The certificate authority decrypts the digital representation and stores it. The registrant then visits a remote registration terminal in person with the digital representation and other identifying documents. The operator of the remote registration terminal verifies the identity of the

registrant from the identifying documents and transmits the digitized representation to the certificate authority. The certificate authority compares the decrypted digital representation with the representation sent from the remote registration terminal. If a match is found, the certificate authority forms a certificate by signing the digital signature using the certificate authority's encrypting key. The certificate is stored in a database and is sent to the registrant. Preferably, the database is public with no restriction as to who may access the stored certificate data. Alternatively, access to the database may be restricted to, for example, employees of a particular corporation or government department, database subscribers, or members of a stock exchange.

According to another aspect of the present invention, the registrant transmits a digital message including the certificate described above. The digital message is then encrypted with the registrant's private encrypting key. The party receiving the encrypted message decrypts the message using the registrant's public decrypting key. The receiving party inspects the message to verify that the appended certificate is valid and that the certificate was prepared by a reputable certificate authority by comparing the certificate with the information stored in the database. The reputation of the certificate authority provides some assurance that the message is genuine and that the sender will not later repudiate the message because his signature and identifying information are part of the certificate stored in the public database.

If additional assurance that the registrant actually transmitted the message is desired, the receiving party can transmit the certificate to the certificate authority and request that the certificate be decrypted to extract the digitized representation. The digital representation is then compared with the digital representation originally submitted by

the registrant. If even greater assurance is required, for example, where the registrant later attempts to repudiate the message, the digital representation can be compared with biological indicia of the registrant from which the digital signature was originally formed.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 shows an embodiment of the invention;

FIG. 2 shows another embodiment of the invention;

FIG. 3 shows another embodiment of the invention;

FIG. 4 shows an embodiment of the invention;

FIG. 5 shows another embodiment of the invention;

FIG. 6 shows another embodiment of the invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

The smart card market is a rapidly growing market. Smart cards are usually divided into two categories: standard smart cards and contactless smart cards. A smart card is a plastic card, having the size of a regular bank or credit card, that contains a semiconductor chip. The International Standards Organization (ISO) specifies the size and thickness of both credit cards and smart cards. The basic contact smart card standard is the ISO 7816 series, part 1-10, while contactless cards will be governed by the ISO 14443 standard. The invention is not limited to systems that implement these standards. The chip in a contactless smart card can store large quantities of information. The card may also contain a microprocessor, which can process data, turning the smart card into a small computer. The smart card is activated by placing the card in a terminal that can

read and write data to/from the card. Standard smart cards must be physically contacted by the terminal for data to be read or written. Contactless smart cards, however, can be accessed without physical contact. Instead, data can be exchanged via radio frequency technology, which is usually 13.56 MHz. To make this possible, a contactless smart card must contain not only a memory and/or a PCU unit but also a transmitter/receiver unit which modulates/demodulates the data and an antenna connected to the chip to transmit/receive the data. The invention is not limited to systems that use the radio frequency bands. The system may use other communication frequency bands.

Wireless communication devices, such as cellular phones and PDAs, are common portable communications devices. There is a need to provide smart card transaction capabilities in these portable devices and to upgrade these wireless communications devices to accommodate smart card transactions. In an embodiment of the invention, a smart card reader/writer module may be provided as an attachment to a standard wireless device. The module may operate at 13.56 MHz high-frequency standard. The module may be appropriately sized to ergonomically match a host wireless device. For example, the module may be approximately 5 cm long, 2-4 cm wide, 4 cm high. The module may be connected to device 220, as shown in FIG. 2, via an interface connector such those used for connecting to regular data modems. In an alternative embodiment, module 210, as shown in FIG. 2, may be integrated into the battery of device 220. In another alternative embodiment, the module may be incorporated into the wireless device 220.

As shown in FIGS.2 and 3, module 210 may be a separate add-on device for connecting to a wireless communication device 220. Module 210 may be connected to communication device 220 through an external connector and may receive power from

a battery (not shown) in communication device 220. In an alternative embodiment, a power supply (not shown) may be included in module 210. The module power supply may also be used as a reserve power supply for communication device 220.

A user may request to receive a biometric authorization smart card from a service center or bank. In a preferred embodiment, the user may visit the service center or bank to initialize the smart card. The user may be required to present at least one form of identification (e.g., driver's license, passport, birth certificate) to the service provider or bank before receiving the smart card. As shown in FIG. 1, the biometric authorization smart card (105) may have a signature scratch pad (110) on the back of the card, which the user may initialize by signing the scratch pad X number of times. For example, the user may be requred to sign the scratch pad three times in front of the bank officer. Once the signature has been applied to the back of the smart card, the signature will be stored in a digital form on a microchip in the card. This has the advantage of eliminating the need for a remote storage center for the biometric information of the user.

With today's advancing technology, there is a growing concern over the collection of personal information such as biometric information for databases, which can be sold to other companies or the government without an individual's knowledge. The growing concern over Big Brother has provided a need for the invention shown herein, where the biometric information is stored in the card and the individual is always in possession of that card. This embodiment elimates the concerns regading the collection of personal biometric information for a centralized database.

After a user has obtained and intialized a biometric authorization smart card, the user or card holder may purchase goods or services using any type of communication

device. A communcations device may be a landline telephone, a wireless device, or a computer capable of exchanging data with another communications device. Figure 6 shows a flow chart of a method of using the biometric smart card. A card holder may establish a communication link via a wireless personal device with another party or service provider (605). It should be noted that any type of communication device may be used to establish a communication link with another party. This may include landline telephones, wireless communication devices, and computer related communication devices, so long as the communication device is equipped to read the biometric authorization smart card.

Once the card holder has established communications with a service provider, the card holder will select an action to be taken with the service provider, such as the purchase of goods and services (610). After a user has decided initiate a purchase, the card holder may select a form or method of payment (615). The method of payment may be integrated into the biometric card or separate from the biometric card. For example, the scratch pad may be associated with a bank credit card which may only be used when the correct signature is applied to the scratch pad at the time of purchase.

In an alternative embodiment, the card may be used as a biometric authorization system for different accounts that have been established with different service providers. The card holder may be requested to sign his/her name with an inkless pen or stylus on the electronic scratch pad of the smart card (620). The scratch pad may be electrically connected to a smart card chip integrated within the biometric authorization smart card (625). This may also be seen in FIG. 6.

The smart card chip may read and analyze the data from the pressure-sensitive

area (i.e., the scratch pad) (630). The smart chip may perform a comparison between the signature stored in the smart chip and a "live" signature to provide positive user authentication and non-repudiation.. For security, the signature pattern stored in the smart chip will be encrypted in the chip's memory. The smart chip internally performs a comparison between the stored signature and the "live" signature of the card holder received from the scratch pad (635).

A threshold level may be set to determine the accuracy of the "match" between the stored signature and the "live" signature. If the comparison yields a result above a pre-defined threshold, the chip may enabled the transaction by transmitting a signal to the vendor. The signal may be as simple as a yes or no response. Alternatively, the signal may be an encrypted form of the signature. Then the card holder will be able to complete the transaction. If the comparison fails to yield a match, the card holder may not be able to complete the transaction.

In an embodiment of the invention, when the comparison fails, a user may either repeat the signature and authentication process or give an alternative identification such as a PIN (using the communications device) or any other method, in order to complete the transaction.

Device 320 may communicate with module 310 via a modem 305. The module may be controlled by central processor unit (PCU) 315, which may be connected to modem 305. PCU 315 may control activity indicators 325 such as transmission/reception activity and on/off status. In addition, PCU 315 may control a display (not shown), which may be located in module 310, in device 320 or both. In another embodiment, module 310 may share a PCU 315 located in device 320.

Module 310 may also be equipped with encryption/decryption unit 335, which may be controlled by the PCU 315. The encryption/decryption unit 335 is used to prevent a third party from intercepting the data transferred to and from the contactless card. The information exchanged between the smart card and the module/device may be encrypted according to various well-documented methods. In one embodiment, the card may authenticate the card reader/writer by generating a random number and sending it to the reader/writer. The reader/writer has to encrypt the random challenge (number) with a shared encryption key and return the result to the card. The card then compares the returned result with its own encryption before agreeing to communicate with the reader/writer. Conversely, the card reader/writer may also authenticate the card's identity by sending a random challenge (number) to the card. The card is then required to sign the number with its own private key, which is part of a private key/public key pair, and return it to the reader/writer for verification.

Furthermore, module 310 may include a radio frequency (RF) unit 345 connected to PCU 335. RF unit 345 may include: (1) a down converter coupled to a low noise amplifier for converting received RF signal waveforms to intermediate frequency (IF) waveforms; (2) an up converter coupled to a high power amplifier for converting modulated analog waveforms from an IF to an RF for amplification and transmission to the antenna; (3) a first analog to digital converter having an input connected to the down converter, for converting the analog IF waveform to a series of digital samples; and/or (4) a first digital to analog converter connected to the up converter for converting modulated digital samples from the processor board to an IF frequency.

The RF section/unit 345 may also be coupled to reader/writer antenna 375. A

variety of reader/writer antennas may be used which allow reading and writing distances up to 100mm, but usually between 0-30mm. Reader/writer antenna 375 should not interfere with the functionality of the device 320. The contactless reader/writer may be provided by companies such as Baltech AG or Tamura Hinchley Ltd.

In an alternative embodiment, the module 10 may be incorporated into the wireless device as shown in FIG. 4. The wireless device may be controlled by the PCU 415, which may control activity indicators 425, such as transmission/reception activity and on/off status. In addition, PCU 415 may control a display (not shown). The wireless device may also be equipped with an encryption/decryption unit 435, which may be controlled by the PCU 415. The device may include two RF units 400 and 445 connected to PCU 415. RF unit 445 may be coupled to reader/writer antenna 475 for providing communication with the smart card. RF unit 400 may provide the traditional voice communications circuitry.

In another alternative embodiment, the module may be incorporated into the wireless device and have only one RF unit. In this embodiment, the voice communications and the smart card transmissions are completed using the same antenna.

In another embodiment, a biometric unit 365/465 may be provided for security purposes. The biometric unit 365/465 may include a biometric input device, such as a fingerprint reader, camera/micro-camera for iris or face recognition, or a standard microphone for voice recognition, to capture biometric information. The biometric unit 365/465 may encrypt the captured data and send it to a remote server or host that will use the data for authentication. Alternatively, the biometric unit 365/465 may perform local authentication and transmit encrypted messages to a host or server, which may be remote.

In another embodiment of the invention, biometric unit 365 may interface with any other biometric reader or any other biometric authentication device.

In another embodiment, when a biometric authentication server receives encrypted biometric data from the device/module the biometric authentication server may be capable of decrypting the data. The biometric authentication server may either identify the owner of the biometric data (one to many) and send the owner's ID data or, when presented 2 sets of biometric data, it replies with either match or no match signal (one-to-one).

During operation, module 10 may be capable of conducting many types of transactions. One example is secure wireless financial transactions. More specifically, the operation of the device 20 may initialize a smart card and/or download an increase in value to a value-holding smart card. The device may also operate to debit value or record a credit transaction for the purchase of merchandise or services. In a typical scenario utilizing module 10 in a commercial purchasing transaction, the user may establish communications with a retailer/host. Once communications are established, the user may be able to receive and preview specially formatted graphical advertisements within display, such as for the purchase of a specific consumer good, or the user may define the required items to be purchased. The host may require the user to identify himself. This may be accomplished by authentication (by a PIN or any Biometric method such as voice, finger print, iris, face, etc.). If authorization is completed, the host computer decreases the stored money amount by the price of the item purchased.

In an embodiment of the invention, the module 10 may be used to purchase and download tickets or other tokens. A user may purchase tickets or tokens that may be

downloaded onto the smart card for storage. Once the user arrives at an event, the user may use the smart card as the admission ticket eliminating the need for a paper ticket. The user of the card will gain entry permission by presenting the contactless card near a local contactless card reader/writer. One smart card can be used to store at least one ticket or token that may be redeemed at places such as movie theaters, stadiums, airline gates etc. Restrictions may be provided that limit the download of tickets or tokens to a contactless smart card from selected wireless devices. In addition, or alternatively, remotely purchased items may be represented by tokens placed on the smart card (contact or contactless). The tokens may be redeemed at any redemption point, such as a store or other distribution station or delivery services for merchandise or services represented by the token. Once the ticket has been redeemed, the ticket maybe marked as unusable or removed from the memory of the smart chip.

Advantageously, the redemption point may also include a biometric unit which can be used in coordination with the biometric data to authenticate redemption of the ticket, token, or debit of the value from the smart card.

In another embodiment, the contactless smart chip may contain an RF unit to be able to communicate with the wireless device directly via the cellular or wireless communication frequency without utilizing a contactless reader/writer at all. Alternatively, the wireless device or add-on device may be adapted to transmit/receive or read/write commands over its principle antenna at an appropriate frequency for the smart cards. A smart card may be restricted to be used only with a predefined cellular phone or a group of cellular phones or other wireless device or with a predefined user over any device. If an authorization program fails to match a card and a device or a card

and a user, services or data transmission/reception may be denied. Alternatively, the authorization program may allow the card the flexibility to work with a group of wireless devices. This method provides an additional level of security and flexibility. It should understood that the RF communication between the communication device and the contactless card may be accomplished using the Bluetooth Standard. The present invention may also be incorporated into a contact card.

We claim:

1. A wireless communication device comprising:

a communications interface;

a contactless smart card interface connected to the communications interface.

2. A wireless communication device according to claim 1 wherein the communications interface further comprising:

a controller;

a transmission/reception subsystem;

a user interface.

3. A wireless communication device according to claim 1 wherein the contactless smart card interface is a contactless smart card read/writer.

4. A wireless communication device according to claim 1 wherein the contactless smart card interface is integrated into the wireless communication device.

5. A wireless communication device according to claim 1 wherein the contactless smart card interface is an add-on module connected to the wireless communication device.

6. A wireless communication device according to claim 1 further comprising:

an authentication subsystem.

7. A wireless communication device according to claim 2 wherein the smart card interface further comprising a reader/writer antenna.

8. A module for a communication device according to claim 6 further comprising a biometric unit.

9. A module for a communication device according to claim 8 wherein the biometric unit further comprising an input unit and output unit.

10. A method for providing wireless communications:

purchasing an item using a wireless communication device and purchasing medium;

providing a security feature to verify a user identification;

delivering the item electronically and storing the item on the purchasing medium.

11. A method for providing wireless communications according to claim 7, further comprising the step of:

redeeming the item stored on the purchasing medium.

12. A method for providing wireless communications according to claim 7, further comprising the step of:

verifying biometric information of the user.

13. A financial information and transaction system comprising:

a host financial computer system, said host system maintaining records of user account information;

a wireless communication device for accessing said host financial computer system, wherein comprising first means for wirelessly transmitting and receiving data, and a contactless smart card reader; and

wherein data corresponding to said user account information is exchanged between said host system and said wireless communication device, such that a user obtains information and performs transactions on said host financial system through a contactless smart card device that is coupled to said contactless smart card reader, said contactless smart card device including means for encrypting data which is exchanged with said host financial system.

14. A method for providing wireless communications comprising the steps of:

capturing biometric data using a wireless device;

performing an authorization to verify a user identification.

15. A method for providing wireless communications according to claim 14 wherein the contactless smart card interface is a contactless smart card read/writer.

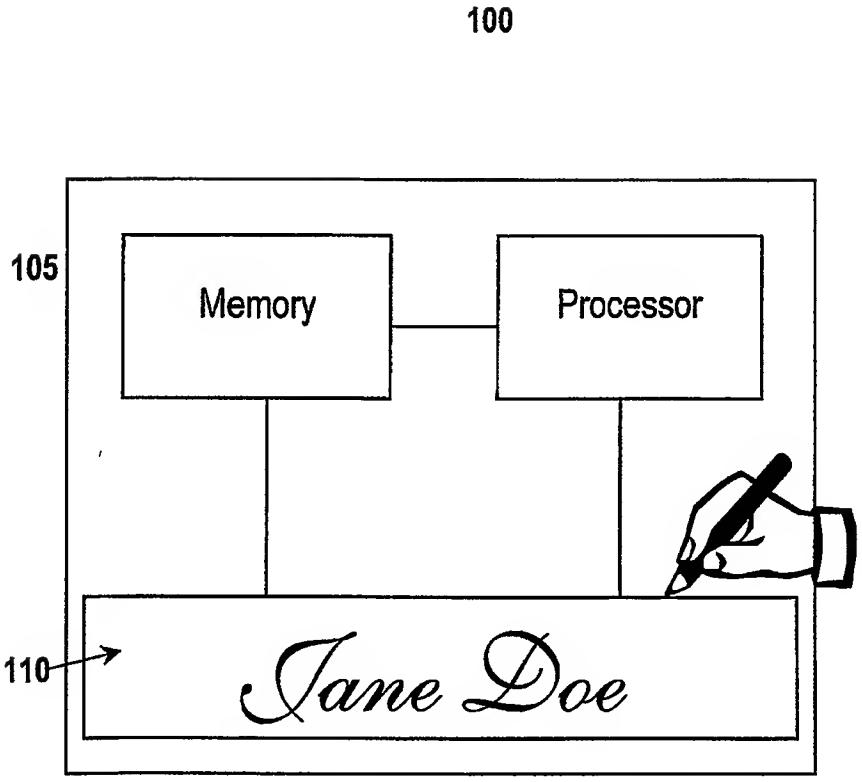


FIG. 1

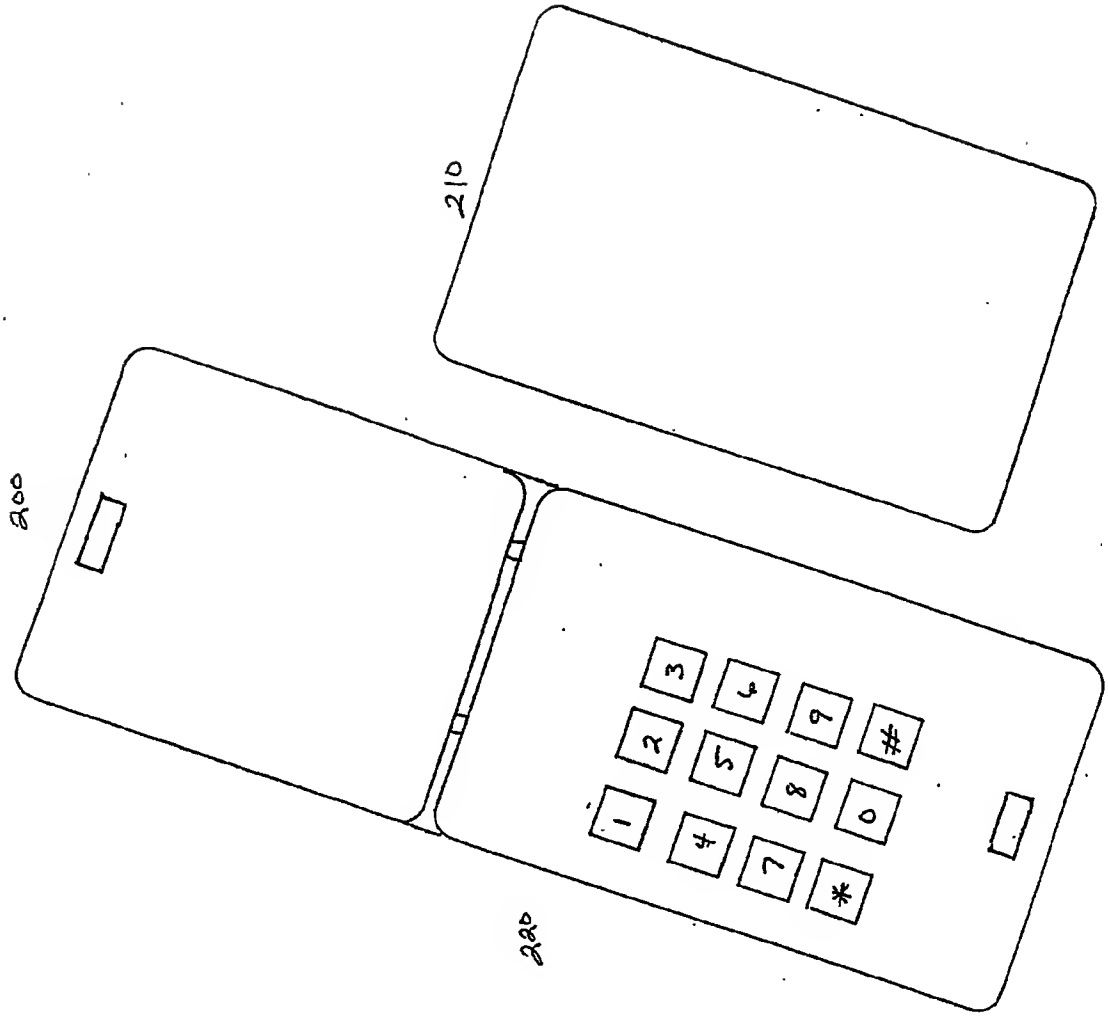


FIG 2

FIG. 3

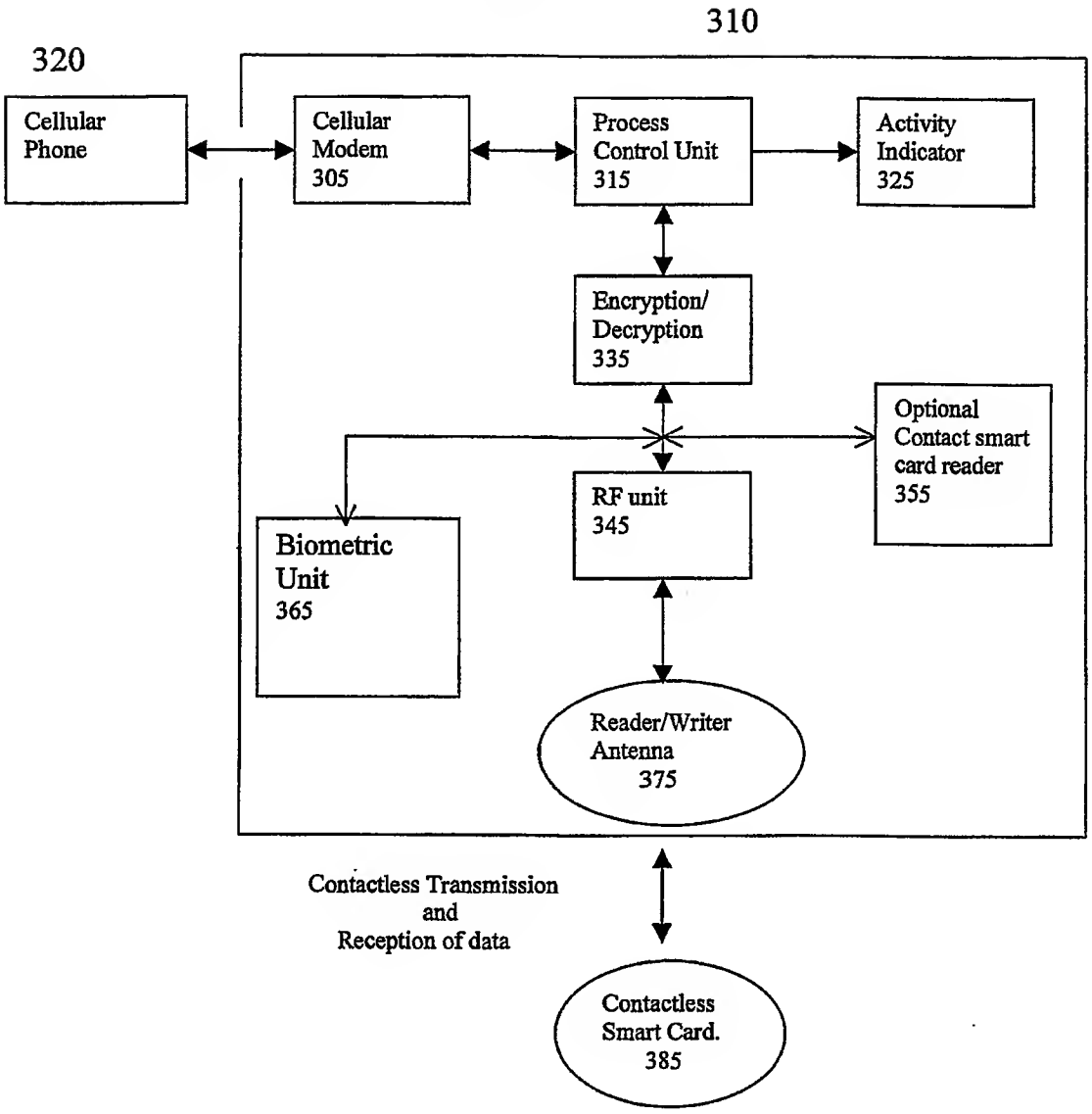
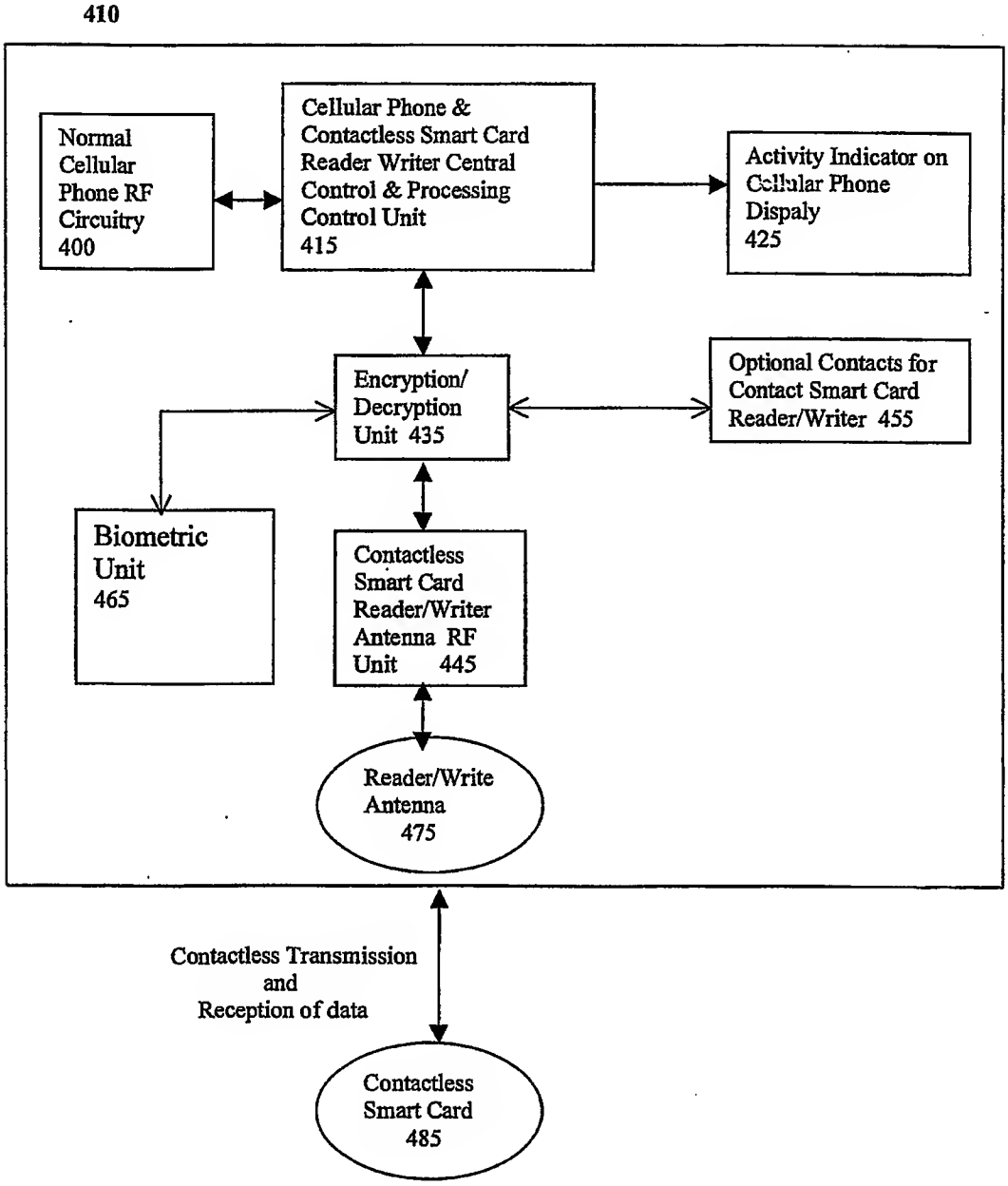

310
320
Cellular Phone
Cellular Modem 305
Process Control Unit 315
Activity Indicator 325
Encryption/ Decryption 335
Optional Contact smart card reader 355
RF unit 345
Biometric Unit 365
Reader/Writer Antenna 375
Contactless Transmission and Reception of data
Contactless Smart Card. 385

FIG. 4


410
Normal Cellular Phone RF Circuitry 400
Cellular Phone & Contactless Smart Card Reader Writer Central Control & Processing Control Unit 415
Activity Indicator on Cellular Phone Dispaly 425
Encryption/ Decryption Unit 435
Optional Contacts for Contact Smart Card Reader/Writer 455
Biometric Unit 465
Contactless Smart Card Reader/Writer Antenna RF Unit 445
Reader/Write Antenna 475
Contactless Transmission and Reception of data
Contactless Smart Card 485

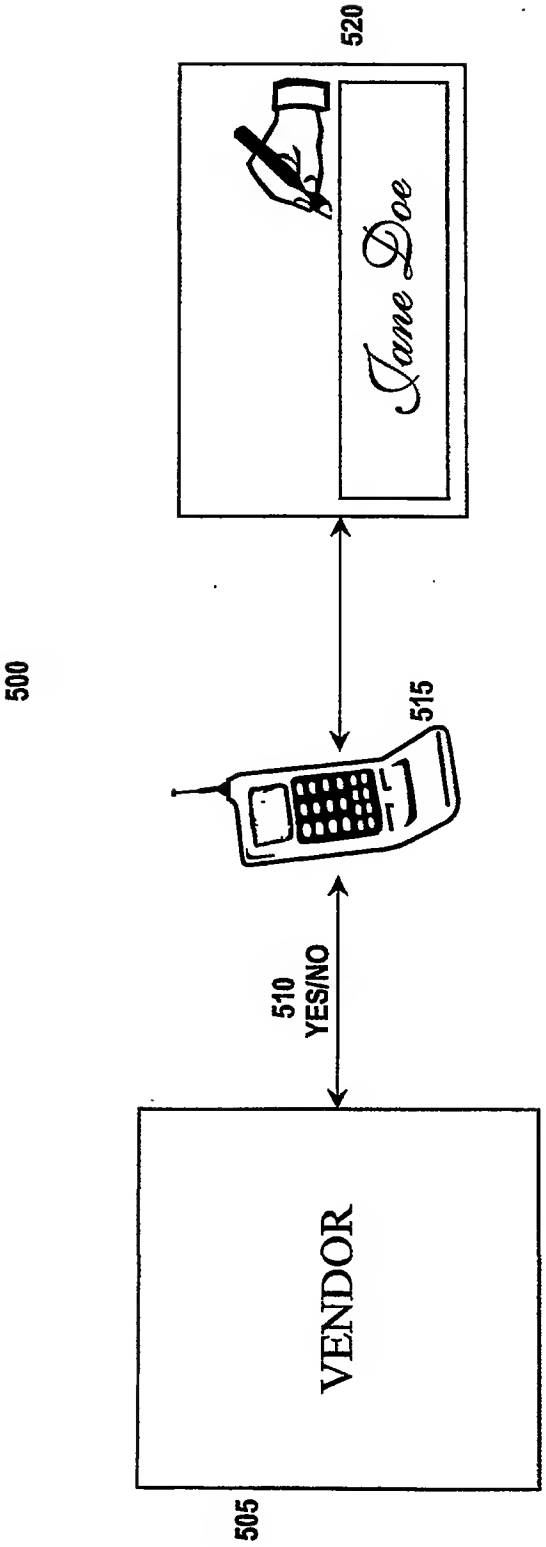


FIG. 5

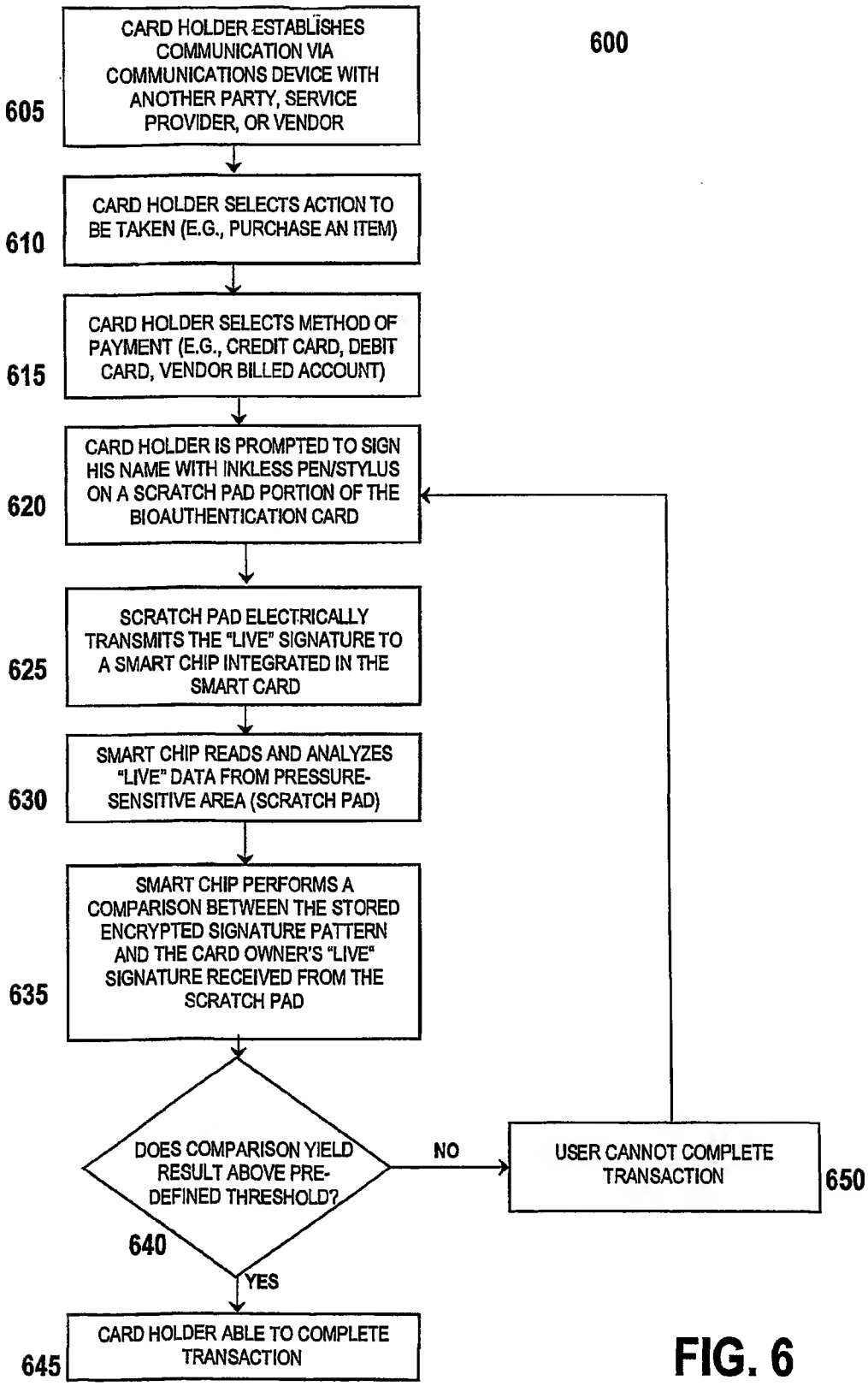

600
CARD HOLDER ESTABLISHES COMMUNICATION VIA COMMUNICATIONS DEVICE WITH ANOTHER PARTY, SERVICE PROVIDER, OR VENDOR
605
CARD HOLDER SELECTS ACTION TO BE TAKEN (E.G., PURCHASE AN ITEM)
610
CARD HOLDER SELECTS METHOD OF PAYMENT (E.G., CREDIT CARD, DEBIT CARD, VENDOR BILLED ACCOUNT)
615
CARD HOLDER IS PROMPTED TO SIGN HIS NAME WITH INKLESS PEN/STYLUS ON A SCRATCH PAD PORTION OF THE BIOAUTHENTICATION CARD
620
SCRATCH PAD ELECTRICALLY TRANSMITS THE "LIVE" SIGNATURE TO A SMART CHIP INTEGRATED IN THE SMART CARD
625
SMART CHIP READS AND ANALYZES "LIVE" DATA FROM PRESSURE-SENSITIVE AREA (SCRATCH PAD)
630
SMART CHIP PERFORMS A COMPARISON BETWEEN THE STORED ENCRYPTED SIGNATURE PATTERN AND THE CARD OWNER'S "LIVE" SIGNATURE RECEIVED FROM THE SCRATCH PAD
635
DOES COMPARISON YIELD RESULT ABOVE PRE-DEFINED THRESHOLD?
640
NO
USER CANNOT COMPLETE TRANSACTION
650
YES
CARD HOLDER ABLE TO COMPLETE TRANSACTION
645

FIG. 6

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 November 2001 (15.11.2001)

PCT

(10) International Publication Number
WO 01/86599 A3

(51) International Patent Classification[7]: G07F 7/10

(21) International Application Number: PCT/IB01/00809

(22) International Filing Date: 13 April 2001 (13.04.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/197,775 14 April 2000 (14.04.2000) US
60/264,013 26 January 2001 (26.01.2001) US

(71) Applicant *(for all designated States except US)*: **SUPER-COM LTD.** [IL/IL]; Hataas Street 25, New Industrial Area, 44425 Kfar Saba (IL).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **LANDMAN, Avi** [IL/IL]; 99 Hagdud Haivri Street, 26306 Kiriat Haim (IL). **ROZEN, Eli** [IL/IL]; 38 Heleni Hamalka Street, 46768 Herzliya Pituah (IL). **HASSAN, Jacob** [IL/IL]; 21 Shnat Hayovel Street, 45304 Hod Hasharon (IL).

(74) Agent: **BEN-DAVID, Yirmiyahu, M.**; Jeremy M. Ben-David & Co. Ltd., P.O. Box 4508, Har Hotzvim Hi-Tech Park, 91450 Jerusalem (IL).

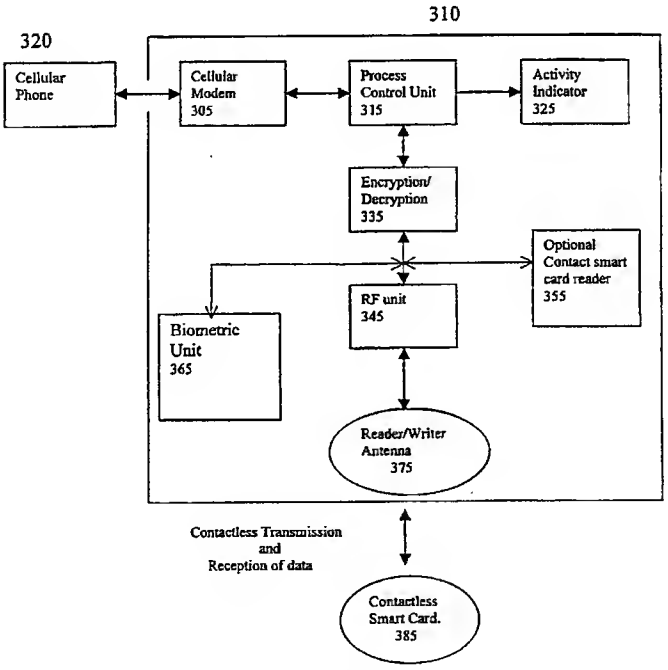
(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CR, CU, CZ, DE, DK, DM, DZ, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

[Continued on next page]

(54) Title: SMART COMMUNICATIONS



(57) Abstract: A method and apparatus for providing a wireless device with the ability to have secure e-commerce transactions utilizing a contactless smart card. Additionally, the method and apparatus provide for a wireless smart card transaction system which utilizes biometric identification methods. The system may incorporate at least one biometric input device, such as a fingerprint reader, a camera or micro-camera for iris or face recognition, and/or a standard microphone for voice recognition or any other biometric input device.

WO 01/86599 A3

— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(88) Date of publication of the international search report:
20 June 2002

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

Inte ..ional Application No
PCT/IB 01/00809

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F7/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 G07F G06K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	EP 0 933 733 A (CITICORP DEV CENTER INC) 4 August 1999 (1999-08-04) paragraph '0012! - paragraph '0015! paragraph '0021! - paragraph '0026! figures 1,7-9 ---	1-15
X	WO 99 53449 A (BASHAN ODED ;GILBOA RONNIE (IL); ADUK MOSHE (IL); ITAY NEHEMYA (IL) 21 October 1999 (1999-10-21) page 8, line 18 -page 9, line 16 page 10, line 13 - line 29 page 12, line 22 -page 13, line 12 figures 1A,3 --- -/--	1-7, 10-13

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 April 2002	02/05/2002

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Papastefanou, E

INTERNATIONAL SEARCH REPORT

Int. ..ional Application No
PCT/IB 01/00809

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
X	WO 98 58510 A (RITTER RUDOLF ;SWISSCOM AG (CH)) 23 December 1998 (1998-12-23) page 5, line 17 -page 8, line 15 page 14, line 15 -page 17, line 8 figure 1	1-7,10, 11,13
A	WO 96 38814 A (PHILIPS ELECTRONICS NV ;MIKRON GES FUER INTEGRIERTE MI (AT); BERGE) 5 December 1996 (1996-12-05) page 4, line 21 -page 6, line 12; figure 1	1-9
A	WO 98 16908 A (DATELNET SMART SERVICES B V ;SENGERS ANTONIUS JOHANNES (NL); SNEL) 23 April 1998 (1998-04-23) page 3, line 30 -page 4, line 30 page 6, line 30 -page 8, line 12 figure 1	1-15

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/IB 01/00809

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
EP 0933733 A	04-08-1999	EP 0933733 A2	04-08-1999
WO 9953449 A	21-10-1999	AU 3165799 A	01-11-1999
		CA 2327728 A1	21-10-1999
		EP 1070302 A1	24-01-2001
		WO 9953449 A1	21-10-1999
WO 9858510 A	23-12-1998	WO 9858509 A1	23-12-1998
		AT 212774 T	15-02-2002
		AU 736350 B2	26-07-2001
		AU 3022497 A	04-01-1999
		AU 739465 B2	11-10-2001
		AU 5649598 A	04-01-1999
		WO 9858510 A1	23-12-1998
		CN 1260939 T	19-07-2000
		DE 59802969 D1	14-03-2002
		EP 0990355 A1	05-04-2000
		EP 0990356 A1	05-04-2000
		HU 0003157 A2	29-01-2001
		HU 0003565 A2	28-03-2001
		NO 996145 A	16-02-2000
		NO 996148 A	11-02-2000
WO 9638814 A	05-12-1996	CN 1172542 A	04-02-1998
		EP 0774144 A2	21-05-1997
		WO 9638814 A2	05-12-1996
		JP 10505932 T	09-06-1998
		US 6168083 B1	02-01-2001
WO 9816908 A	23-04-1998	NL 1004249 C2	15-04-1998
		AU 720416 B2	01-06-2000
		AU 4474297 A	11-05-1998
		EP 1012798 A1	28-06-2000
		WO 9816908 A1	23-04-1998